Deutscher Bundestag **Drucksache 17/8257**

17. Wahlperiode 21. 12. 2011

Kleine Anfrage

der Abgeordneten Andrej Hunko, Jan Korte, Herbert Behrens, Nicole Gohlke, Annette Groth, Dr. Rosemarie Hein, Ulla Jelpke, Niema Movassat, Jens Petermann, Dr. Petra Sitte, Alexander Ulrich, Kathrin Vogler und der Fraktion DIE LINKE.

Computergestützte Kriminaltechnik bei Polizeibehörden

Die Aufrüstung computergestützter Ermittlungsmethoden schreitet rasant voran. Die Anstrengungen auf Bundes- und Landesebene werden seit 2007 auch auf Ebene der Europäischen Union (EU) vorangetrieben: Auf Initiative des ehemaligen Bundesinnenministers Dr. Wolfgang Schäuble hatten sich einige europäische Innenminister in der sogenannten Future Group organisiert, um bei Weichenstellungen zukünftiger Polizeiarbeit mitzureden. Schon damals wurde von „gewaltigen Informationsmengen, die für öffentliche Sicherheitsorganisationen nützlich sein können“ orakelt: Der erwartete „Digitale Tsunami“ würde demnach verheißen, Milliarden elektronischer Geräte in Echtzeit zu verfolgen und Verhaltensmuster ihrer Nutzer und Nutzerinnen zu analysieren.

Die Proteste gegen die Naziaufmärsche in Dresden Anfang 2011 sorgten zudem für mehr Bewusstsein in Bezug auf die polizeiliche Nutzung von Daten aus der Funkzellenauswertung (FZA). Die Daten werden ebenfalls von einer Software aufbereitet und analysiert, bevor sie einer Software zur Auswertung zugeführt werden. Diese in Polizeikreisen sogenannte telekommunikative Spurensuche kann aber auch in Echtzeit genutzt werden, wie es bereits 2009 über eine Plattform von Nokia Siemens Networks im Iran berichtet wurde: Die staatlichen Milizen registrierten Spontanversammlungen über auffällig viele Mobiltelefone in Funkzellen. In Deutschland kommt hierzu ein sogenannter International Mobile Subscriber Identity (IMSI)-Catcher zur Anwendung, mit dem Standort- und Verbindungsdaten eines zuvor ermittelten Mobiltelefons innerhalb einer Funkzelle eingegrenzt wird (Bundestagsdrucksache 17/7652).

Neben der seit langem üblichen Vorgangsverwaltung setzen Polizeien Ermittlungssoftware ein, die Beziehungen unter polizeilichen Datensätzen finden soll. Aufgebohrt mit Zusatzmodulen werden etwa in der Anwendung rsCase der deutschen Firma rola Security weitere Datenquellen angeschlossen, GPS-Tracker eingebunden oder per Onlineschnittstelle Daten aus der Telekommunikationsüberwachung (TKÜ) eingespielt. Die Suche nach Auffälligkeiten wird als „Data Mining“ bezeichnet und soll einen Mehrwert aus bislang unstrukturierter Information verschaffen. Die Software-Industrie bietet statistische Verfahren für die Polizeiarbeit an, die mittels „vorausschauender Analyse“ Kriminalitätsmuster erkennen und sogar Straftaten vorhersehen will.

Auch das Internet wird mit IT-Anwendungen ausgeforscht. Telekommunikationsanbieter sind zur Zusammenarbeit mit Verfolgungsbehörden verpflichtet

und müssen hierfür technische Standards für „Lawful Interception“ (etwa: behördliches Abhören) einhalten. Von den Providern herausgegebene Daten werden automatisiert übertragen und ausgewertet. Weil immer mehr Nutzer und Nutzerinnen allerdings ihre Kommunikation verschlüsseln, infiltrieren Polizeien und Geheimdienste die genutzten Rechner direkt mittels staatlichen Trojanern. Auch die hierüber erlangten Rohdaten werden mittels Software automatisiert ausgewertet.

Die Überwachung des Nutzerverhaltens im Internet bleibt indes nicht auf den eigenen Rechner beschränkt. Soziale Netzwerke müssen ebenfalls Daten an Verfolgungsbehörden herausgeben. Zudem können die von den Nutzern angelegten Profile auch ohne richterlichen Beschluss computergestützt durchforstet werden. Auch in Blogs und Chaträumen kann nach Verhaltensanomalien, Interessen von Gruppen, Trends oder anderen Aussagen über Beziehungen zwischen Personen und Vorgängen gesucht werden.

Die Menge an Daten aus Videoüberwachung, Funkzellenauswertung, Peilsendern oder auch der Auswertung des Internets erfordert nicht nur gehörige Investitionen in breitbandige Netzwerke, Endgeräte oder Speichermedien. Vielfach laufen die Information in Lagezentren zusammen. Zur Visualisierung eingehender Informationen sollen Monitoring Centres den Behörden ein umfassendes Lagebild verschaffen und die Entscheidungsfindung und Führungsfähigkeit verbessern.

Die polizeilichen Begehrlichkeiten nach digitalen Kriminalwerkzeugen sind längst nicht gestillt. Dass stets nach neuen auszuspähenden Kommunikationsmitteln gesucht wird, belegt der kürzlich geleakte „Leitfaden zum Datenzugriff“ der Staatsanwaltschaft München (www.vorratsdatenspeicherung.de/images/leitfaden_datenzugriff_voll.pdf). Demnach nutzen die Behörden neben „Stillen SMS“ und IMSI-Catchern zum Lokalisieren von Mobiltelefonen auch das „eTicketing“ der Deutschen Bahn, um Verdächtige auszuspähen.

Um überhaupt einen Überblick zu kriminalistisch genutzter Digitaltechnik zu erlangen, ist ein Einblick in die Funktionsweise obligatorisch. Hierzu muss die Öffentlichkeit auch über deren Hersteller informiert sein. Sofern Daten verarbeitet werden, die tief in die Privatsphäre eingreifen oder Anwendungen sogar auf deren Grundlage Risikoanalysen erstellen wollen, muss zudem der Quellcode der Software offen gelegt werden. Diesen unter Verweis auf geschützte „Vermögenswerte“ der Hersteller zu verweigern (vgl. Bundestagdrucksache 17/7760), wird von dem Fragesteller nicht hingenommen.

Wir fragen die Bundesregierung:

1. Welche gesetzlichen Regelungen gelten für in Deutschland ansässige Telekommunikationsfirmen, Netzbetreiber und Serviceanbieter hinsichtlich der Überwachung von Telekommunikation?

   a) Welche Behörden der Bundesregierung (auch des Verfassungsschutzes) beteiligen sich seit wann an der internationalen Arbeitsgruppe Technical Specification Group Services and System Aspects; 3G Security; Lawful Interception Requirements?

   b) Welche Behörden der Bundesregierung (auch des Verfassungsschutzes) beteiligen sich an welchen anderen nationalen oder internationalen Arbeitsgruppen zu Standards für Lawful Interception (Standardisierungsgremien)?

   c) Mit Vertretern welcher deutscher Firmen arbeiten Bundesbehörden desweiteren bezüglich internationaler oder deutscher Standards für Lawful Interception zusammen?

d) Mit dem Abhören welcher Technologien haben sich die oben genannten Treffen bzw. Arbeitsgruppen befasst?

e) Welchen Bedarf sieht die Bundesregierung zur Ausgestaltung zukünftiger Werkzeuge zur Telekommunikationsüberwachung, und welche Prognosen bzw. Studien liegen hierfür vor?

2. Wie wird die deutsche Telekommunikationsüberwachungsverordnung von 2002 durch die Bundesbehörden konkret umgesetzt?

a) Welche Bundes- und Landesbehörden und gesetzgebende Körperschaften sind zur Ausführung von TKÜ berechtigt?

b) Welche weiteren berechtigten Stellen können derartige Überwachungsmaßnahmen beantragen oder erlassen?

c) Welche Gerichtsbeschlüsse oder richterlichen Anordnungen sind für welche Maßnahmen jeweils erforderlich, bzw. in welchen Fällen reicht eine Anordnung durch die Staatsanwaltschaft oder einer anderen Behörde?

d) Wie werden TKÜ-Maßnahmen auf Rechtsgrundlage der Strafprozessordnung von solchen zur Gefahrenabwehr voneinander abgegrenzt, bzw. welcher Unterschied ergibt sich hieraus für die Provider?

e) Welche Rechtsgrundlage bieten die Bestimmungen des BKA oder des Bundespolizeigesetzes (BPolG) für eine TKÜ-Anordnung zur Gefahrenabwehr?

3. Wie setzen sich die Kosten für eine Telekommunikationsüberwachung im Einzelfall zusammen?

a) Welche Kosten entstanden den Referaten des Bundeskriminalamtes (BKA) Einsatz- und IT-Unterstützung (im Bereich Organisierte Kriminalität – OK), Einsatz- und IT-Unterstützung (beim Staatsschutz), TKÜ und Mobilfunkforensik in den letzten fünf Jahren im Rahmen von Abhörmaßnahmen, und wie standen diese im Verhältnis zum Gesamtetat?

b) Mit welchen Interception Service Providern arbeiten Bundesbehörden zur Umsetzung von Lawful-Interception-Aufträgen zusammen?

c) Welche Dienste werden in diesem Falle über Interception Service Provider ausgelagert (etwa Mietgeräte und Leihausrüstungen, technischer Support oder Managed Services)?

d) Ist es Bundesbehörden – wie vom Abhördienstleister Utimaco berichtet – technisch möglich, die Ausforschung etwa einer einzigen E-Mail oder einer bestimmten Absenderadresse in großen Internetknoten wie DE-CIX zu gewährleisten oder werden derartige Dienste an private Firmen ausgelagert?

4. Welche digitalen Anwendungen zur Lawful Interception werden für leitungsvermittelnde Netze, paketvermittelnde Netze, Funknetze, Übertragungswege für teilnehmerbezogenen Internetzugriff und Breitbandkabelnetze durch Bundesbehörden bzw. die hierzu verpflichteten TKÜ-Provider jeweils genutzt?

a) Welche Hardware welcher Anbieter kommt hierfür seit wann zum Einsatz?

b) Welche Software welcher Anbieter kommt hierfür seit wann zum Einsatz?

c) Welche Übergabeschnittstellen zu Providern werden betrieben bzw. genutzt?

d) Welche Behörden betreiben Server zum Ausleiten bzw. Empfangen von Daten aus der TKÜ durch Provider?

e) In welchen Fällen wurden oder werden Daten auf Datenträgern, etwa USB-Sticks oder gebrannte Datenträger, weitergegeben, und wie ist das Procedere hierzu?

5. Wie ist rechtlich und technisch umgesetzt, dass eine Anfrage zur TKÜ in Echtzeit bei den Providern unverzüglich aktiviert wird?

a) Wie greifen Bundesbehörden in Echtzeit bzw. nahezu Echtzeit auf Informationen aus der TKÜ zu?

b) Über welche Übertragungsverfahren wird eine Übermittlung in Echtzeit bewerkstelligt?

c) Welche Hard- und Software welcher Hersteller kommt für die gesamte Echtzeitmaßnahme (auch für die Auswertung der Daten) auf den Seiten von Bundesbehörden jeweils zum Einsatz?

d) Wie viele Echtzeitüberwachungsaktivitäten der TKÜ können von den bei den Bundesbehörden genutzten Plattformen jeweils gleichzeitig verarbeitet werden?

6. Wie wird bei den genutzten technischen Anwendungen sichergestellt, dass sensible private Daten während der Übertragung zur ausforschenden Behörde geschützt werden, und welche Verschlüsselungsverfahren kommen hierbei zur Anwendung?

a) Welches private oder behördliche Personal ist dazu autorisiert, die im gesamten Prozess anfallenden Überwachungsdaten einzusehen?

b) Wie werden TKÜ-Aktivitäten protokolliert und wo werden diese Protokolle abgelegt?

c) Wie wird vor der Inbetriebnahme von Anlagen neuer Telekommunikationsprovider eine Abnahme ihrer Überwachungsausrüstung gewährleistet?

d) Welche Bundes- und Landesbehörden sind zur Prüfung jener Anlagen autorisiert?

e) Wie wird es seitens der einsetzenden Polizeien oder Geheimdienste technisch bewerkstelligt, dass Überwachungsmaßnahmen für die Betroffenen nicht erkennbar sind?

7. Welchen Inhalt hat eine Überwachungsverfügung an den Telekommunikationsanbieter, und auf welchem Wege wird diese zugestellt?

a) Wie viele Anordnungen haben die Bundesbehörden in den Jahren 2010 und 2011 erlassen (bitte nach Monaten aufschlüsseln)?

b) In welcher Zeitspanne muss der Diensteanbieter auf eine Anordnung zur TKÜ reagieren?

c) Welche Möglichkeit hat der Provider, sich gegen eine polizeiliche oder richterliche Anordnung auf Herausgabe von Daten zu wehren?

d) Wie viele entsprechende Anordnungen haben Provider in den letzten beiden Jahren zurückgewiesen (bitte für Facebook, Skype, Google+, Twitter, StudiVZ und Wer kennt wen gesondert ausweisen)?

e) Welche ausländischen Provider arbeiten in der Praxis hinsichtlich sogenannter emergency disclosure request gut mit den Bundesbehörden zusammen, wie es die bayerische Generalstaatsanwaltschaft im „Leitfaden zum Datenzugriff“ etwa für Google, YouTube, Skype, Microsoft berichtet?

8. Welche Anwendungen bevorraten Bundesbehörden zur Analyse von telekommunikativen Daten aus der FZA?

   a) Wie werden die Bestandsdaten nach einer FZA von Providern an Verfolgungsbehörden übermittelt, welche Schnittstellen existieren hierzu, und inwieweit ist dieser Vorgang bereits automatisiert?

   b) Welche Software welcher Hersteller wird hierfür eingesetzt, über welche Funktionalitäten verfügen die Anwendungen, und auf welche Datenbanken oder sonstigen Informationen wird lesend oder schreibend zugegriffen?

   c) Welche Bundesbehörden sind an der kriminaltechnischen Nutzung von Daten aus dem Elektronischen-Ticket-System (e-Ticketing) der Deutschen Bahn interessiert, und welche Initiativen bzw. Treffen mit welchen Firmen haben hierzu bereits stattgefunden?

9. Kann die Bundesregierung, obwohl sie keine Statistiken über die Anwendung der Funkzellenauswertung führen will, für ihre einzelnen Behörden zumindest Angaben über die ungefähre Größenordnung ihrer Anwendung in den letzten fünf Jahren (etwa 1 bis 10 pro Jahr, 50 bis 100 pro Jahr, über 100 pro Jahr) bzw. wenigstens Angaben zu besonderen Tatkomplexen der Vergangenheit machen, anhand derer das Verfahren von polizeilichen Ermittlungen, Antragsstellung durch die Staatsanwaltschaft, richterlichem Beschluss bis hin zur Ausführung und Auswertung der Funkzellenauswertung durch die Fragesteller und Fragestellerinnen nachvollzogen werden kann?

10. Inwieweit sind Bundesbehörden in der Lage, WLAN-Netzwerke mittels W-LAN-Catchern zu überwachen?

    a) Wie ist ihr Einsatz rechtlich geregelt?

    b) Welche Produkte welcher Hersteller wurden hierfür bereits begutachtet, getestet oder kommen zur Anwendung?

    c) Wie oft haben Bundesbehörden in den letzten fünf Jahren von derartigen Geräten Gebrauch gemacht?

11. Welche Anwendungen bevorraten Bundesbehörden zum Versenden von Stillen SMS (im Polizeijargon Ortungsimpulse)?

    a) Mit welchen Anwendungen (Hard- und Software) welcher Hersteller werden die Stillen SMS versandt?

    b) Welche Landes- oder Bundesbehörden verfügen hierzu über (auch gemeinsam genutzte) SMS-Server?

    c) Kann die Bundesregierung Angaben zu besonderen Tatkomplexen der Vergangenheit machen, anhand derer das Verfahren von polizeilichen Ermittlungen, Antragsstellung durch die Staatsanwaltschaft, richterlichem Beschluss bis hin zur Ausführung und Auswertung durch die Fragesteller und Fragestellerinnen nachvollzogen werden kann?

    d) Kann die Bundesregierung exemplarisch schildern, nach welchem Verfahren eine richterliche Anordnung zur TKÜ an den Provider, das Versenden einer Stillen SMS durch die Polizei oder den Geheimdienst, das Ausleiten von derart erzwungenen Standort- oder Bestandsdaten durch einen Provider, das polizeiliche Verarbeiten der erlangten Daten sowie das weitere Versenden Stiller SMS miteinander synchronisiert sind?

    e) Wie ist die Nutzung Stiller SMS rechtlich geregelt, und welche Position vertritt die Bundesregierung hinsichtlich der Frage, ob es sich dabei um einen Kommunikationsvorgang handelt?

f) Wie wird sich die Bundesregierung im Bundesrat positionieren, wenn die Entwicklung strengerer Kriterien für die Anordnung, Durchführung und Protokollierung zukünftiger Maßnahmen zur Funkzellenauswertung oder des Versendens Stiller SMS zur Debatte steht?

g) Welche fachliche Beratung wird von den zuständigen Fachausschüssen des Bundesrates bei welchen Experten hierzu gegenwärtig eingeholt?

12. Welche Bundesbehörden sind zur Nutzung sogenannter IMSI-Catcher berechtigt, und welche rechtlichen Vorgaben liegen dem zugrunde?

a) Welche Hersteller haben Bundesbehörden wann IMSI-Catcher geliefert, und wie wurde die Vergabe jeweils geregelt?

b) Wie viele IMSI-Catcher stehen Bundesbehörden zur Nutzung zur Verfügung, und welche Spezifikationen weisen die Geräte auf?

c) Welche Geräte wurden und werden Bundesbehörden innerhalb der letzten fünf Jahre leihweise überlassen bzw. geleast oder gemietet?

d) Welche Kosten sind für die Beschaffung von IMSI-Catchern in den letzten fünf Jahren entstanden?

e) Welche Geräte wurden wann und aus welchen Gründen aus dem Bestand entfernt?

f) Inwiefern ist es möglich, mittels der Geräte die Kommunikation eines einzelnen Teilnehmers oder einer gesamten Funkzelle zu unterdrücken?

13. Inwieweit können Bundesbehörden GPS-Empfänger unter anderem in Mobiltelefonen oder Navigationsgeräten als Spähwerkzeuge nutzen?

a) Mit welchen Firmen arbeiten Bundesbehörden hinsichtlich LocationBased Service-Diensten zusammen, und welche Anwendungen werden hierfür genutzt?

b) Wie ist die Herausgabe der sensiblen Standortdaten von Überwachten durch den privaten Diensteanbieter geregelt?

c) Welche technischen Möglichkeiten bevorraten Bundesbehörden zur Erlangung oder Herausgabe von Signalen jener GPS-Module, die serienmäßig in Mobiltelefonen eingebaut sind?

d) Inwieweit könnten Mautdaten, die beim automatisierten Abrechnungssystem mittels GPS oder On Board Unit anfallen, technisch genutzt werden, und welche rechtlichen Hürden existieren hierzu?

e) Inwiefern sind Bundesbehörden technisch in der Lage, SIM-Module in Fahrzeugen (etwa Audi-Ortungsassistent Cobra, BMW-Assist/ConnectedDrive oder ähnliche Systeme bei Porsche, Renault und Opel) für polizeiliche Zwecke zu nutzen bzw. welche Überlegungen oder Anstrengungen wurden für eine zukünftige Nutzung unternommen?

14. Welche Software welcher Hersteller kommt bei Bundesbehörden zur kriminalpolizeilichen Vorgangsverwaltung und Fallbearbeitung zur Anwendung zur Anwendung (bitte nach Vorgangsbearbeitung, kriminalistische Fallbearbeitung aufschlüsseln)?

a) Auf welche Polizeidatenbanken oder sonstigen Informationen dürfen die Anwendungen zugreifen?

b) Welche Datenbanksysteme welcher Hersteller liegen den Anwendungen jeweils zugrunde?

c) Welche Zusatzmodule werden hierbei im Regel- oder Einzelfall von der Software eingebunden?

d) Inwieweit können auch GPS-Tracker eingebunden werden?

e) Wie werden TKÜ-Daten von Telekommunikationsprovidern in die Anwendungen eingespielt?

f) Inwieweit kann die genutzte Software einen Mehrwert aus bislang unstrukturierter Information finden?

15. Handelt es sich bei den Systemen zur Vorgangsverwaltung und Fallbearbeitung jeweils um Entwicklungen durch Dritte im Auftrag bzw. für den Einsatzzweck der jeweiligen Behörden, um die Beschaffung (und gegebenenfalls Anpassung) sogenannter Commercial off the shelf-Produkte (COTS) oder um Eigenentwicklungen der Behörden?

a) Welche Kosten sind Bundesbehörden im Einzelfall und unter Berücksichtigung der Arbeitszeit innerhalb der Behörde für die Beschaffung, Anpassung, den Service und Pflege der Software bisher entstanden?

b) Wurden für die Systeme bisher schon Wirtschaftlichkeitsbetrachtungen entsprechend den Empfehlungen des Beauftragten der Bundesregierung für Informationstechnik (CIO Bund) durchgeführt, und wenn ja, mit welchem Ergebnis, bzw. wenn nein, warum nicht?

16. Welches Volumen haben bzw. hatten Lizenz-, Support- und Serviceverträge von Bundesbehörden innerhalb der letzten fünf Jahre mit den Firmen Oracle, Microsoft (Datenbanksystem), Trivadis, Mummert & Partner, Gora. Hecken & Partner und der Valora Management Group?

a) Welche Software der Firma IBM (bitte die Produktbezeichnung angeben) nutzt das BKA wie in der Antwort der Bundesregierung auf Bundestagsdrucksache 17/6587 berichtet „zu Testzwecken“, und welche „einzelfallabhängig unterschiedliche kriminalistische Fragestellungen“ wurden jeweils damit bearbeitet?

b) Wer hat die Initiative zum Test der IBM-Anwendung ergriffen, und welche Kosten fielen für die Beschaffung an?

c) Welche Firmen haben zusammen mit dem BKA im Rahmen der Spezialmesse General Police Equipment Exhibition & Conference 2010 in Leipzig an der Arbeitsgruppe Software-Koordinations-Maßnahmen im Bereich der IT-Forensik teilgenommen?

d) Welche Inhalte wurden in der Arbeitsgruppe Software-Koordinations-Maßnahmen im Bereich der IT-Forensik erörtert (bitte in groben Zügen wiedergeben)?

17. Inwieweit unterscheiden sich beim Bundeskriminalamt Fallbearbeitungssysteme für die eigene operative Arbeit von jenen Anwendungen, die in seiner Rolle als Zentralstelle für kriminalpolizeiliche Informationssysteme für Bund und Länder genutzt werden?

a) Seit wann existieren beim BKA die sogenannte Bund-Länder-Datei-Schnittstelle (BLDS) und die Bund-Länder-Online-Schnittstelle (BLOS)?

b) Worum handelt es sich bei diesen Schnittstellen, und wofür werden sie seit wann, und von wem genutzt?

c) Wer hat diese Schnittstellen entwickelt, und wie war das Beschaffungsverfahren für deren Entwicklung ausgestaltet?

d) In welchem Umfang und für welche Zwecke werden das vom BKA im Rahmen seiner Zentralstellenfunktion gegenüber den Verbundteilnehmern zur Verfügung gestellte Informationssystem Inpol-Fall als Basis für den (derzeitigen) Kriminalpolizeilichen Meldedienst und die Anti-Ter-

ror-Datei sowie die BLDS und die BLOS von den Ländern und anderen Verbundteilnehmern im operativen Einsatz genutzt?

e) Welche Firma oder Behörde hat die Datenbankstruktur von Inpol-Fall sowie die auf diese Datenbank zugreifende Erfassungs- und Abfragesoftware entwickelt bzw. an der Entwicklung mitgewirkt?

f) Wie und in welchem Umfang wurden die Nutzungs-, Bearbeitungs- und Verwertungsrechte des Vorgängersystems namens Crime von Inpol-Fall an das BKA übertragen, und wer war der übertragende Rechteinhaber?

18. Wie grenzt sich das System Inpol-Fall technisch und rechtlich ab von dem unter der Ägide des Inpol Land COmpetence Center (IPCC) bzw. der Hessischen Zentrale für Datenverarbeitung (HZD) weiterentwickelten und ebenfalls als Fallbearbeitungssystem angebotenen Systems Crime?

a) Was hat die Bundesregierung unternommen, um zu prüfen, welche Synergieeffekte sich durch eine Zusammenlegung der Weiterentwicklung und Pflege der zwei sehr ähnlichen Systeme, Inpol-Fall und Crime, erzielen ließen, und welche Ergebnisse hat diese Prüfung ergeben?

b) Stellt die generische Datenbankstruktur des Systems Inpol-Fall und seines Vorgängersystems Crime nach Ansicht der Bundesregierung eine Verletzung des Patents auf die Datenbankstruktur dar, die im System Polygon realisiert ist und im Besitz der Firma Polygon steht?

c) Wie ist der aktuelle Stand der Planung bzw. Umsetzung zur Neuaufstellung des Kriminalpolizeilichen Meldedienstes auf der Basis des geplanten „Polizeilichen Informations- und Analyseverbunds für Bund und Länder (PIAV) (siehe Bundestagsdrucksache 17/5328)?

d) Welche konkreten technischen Prüfaufträge wurden erteilt, um die Möglichkeit zu untersuchen, das vorhandene System Inpol-Fall für die Zwecke von PIAV weiterzuentwickeln bzw. zu erweitern, und zu welchen Ergebnissen hinsichtlich der Machbarkeit, des Zeit- und Kostenaufwands sind diese Prüfungen gekommen?

e) Welche Rolle spielt bzw. spielte nach den Erkenntnissen der Bundesregierung die Gesellschaft für technische Sonderlösungen (GTS) bzw. deren Geschäftsführer als Anbieter bzw. Dienstleister auf dem Gebiet der Lawful Interception?

f) War die Firma GTS oder ihre der Bundesregierung bekannte frühere Mitarbeiter und Mitarbeiterinnen mit der Entwicklung von Trojaner-Software des Bundes beauftragt bzw. daran beteiligt?

19. Seit wann wird das Fallbearbeitungssystem der Firma rola Security beim BKA eingesetzt?

a) Warum nutzt das BKA für die Fallbearbeitung, -analyse und -auswertung im Rahmen seiner eigenen, operativen Aufgaben ein Fallbearbeitungssystem auf der Basis von rsCase der Firma rola Security, und nicht das beim BKA für Zentralstellenaufgaben eingesetzte Informationssystem Inpol-Fall?

b) Wird vom BKA auch die seitens rola beworbenen „automatische Erkennung und Darstellung vorhandener Strukturen zwischen Personen, Organisationen und gemeinsam verwendeter Infrastruktur“ genutzt?

c) Welche Schnittstellen und Module können im Regel- sowie im Einzelfall eingebunden werden?

d) Welche Datenbanken werden von rsCase, bCase oder anderen rola-Produkten abgefragt, wie es von rola als „Einmalerfassung – Mehrfachnutzung“ beworben wird?

e) Welche Verfahren einer „automatischen Datenübernahme“ kommen hierbei zur Anwendung?

f) Wie ist die Nutzung der „Antiterrordatenbank“ oder von Inpol technisch und rechtlich geregelt?

g) Inwieweit können kriminaltechnische Spuren eingebunden werden, und welche weiteren Anwendungen existieren hierzu?

h) Inwieweit kann die genutzte rola-Software über eine Personenrecherche auch biometrische Daten verarbeiten?

i) Welche Module existieren zur Erhebung und Einbindung von Geodaten?

j) Haben das BKA oder andere Bundesbehörden jemals vom Data Mining- und Statistik-Modul von der rola-Software Gebrauch gemacht?

k) Inwieweit kann die beim BKA genutzte rola-Software für Maßnahmen in Echtzeit genutzt werden?

l) Wie ist es technisch umgesetzt, dass für neu eingegangene Informationen eine Meldung ausgegeben werden kann?

m) Wie ist das Berechtigungskonzept innerhalb von rsCase bzw. ähnlicher Anwendungen geregelt, und wer trifft im Ermittlungsfall die jeweiligen Bestimmungen hierzu?

20. Wie wurde die Vergabe und Beschaffung von rola-Software in den letzten zehn Jahren geregelt?

a) In welchen Fällen wurde rola-Software ohne Vergabebekanntmachung beschafft, und wie wurde das Verfahren im Einzelnen begründet?

b) Welche Kosten entstehen für den technischen Betrieb, Wartung und Pflege von rola-Software, und wer führt diese aus?

c) Welche Kosten sind im Einzelfall für die Beschaffung von Zusatzmodulen entstanden?

d) Welche weiteren laufenden Kosten fallen an?

e) Welche Errichtungsanordnungen existieren zu den einzelnen rola-Anwendungen?

21. Seit wann gilt rsCase als „bundesweit abgestimmtes Kerndatenmodell“ unter den Ländern (Sächsischer Landtag, Drucksache 5/6190)?

a) In welchen länderübergreifenden Arbeitsgruppen wird die Nutzung von rola-Software durch Polizeibehörden begleitet oder ausgewertet?

b) Trifft es zu, dass das BKA in seiner Rolle als Zentralstelle den Ländern für bund-/länderübergreifende gemeinsame Ermittlungen, z. B. im Staatsschutz, den Einsatz von rsCase bzw. bCase empfiehlt oder sogar für den Datentausch vorgibt?

c) Falls ja, aufgrund welcher technischer und wirtschaftlicher Erwägungen wird rola-Software gegenüber anderen Produkten bevorzugt?

d) Trifft es zu, dass das beim BKA eingesetzte bCase keine Informationen an Inpol-Fall weitergeben kann, und falls ja, welcher einmalige und laufende Aufwand entsteht dem BKA durch eine etwaige Mehrfacherfassung von Daten in beiden Systemen?

22. Seit wann nutzt das BKA das Violent Crime Linkage Analysis System (ViCLAS), und wie wurde die Beschaffung geregelt?

    a) Mit welcher Zweckbestimmung wurde das System errichtet?

    b) Auf welche Datenbestände greift ViCLAS im Einzel- und im Regelfall zu?

    c) Welche Kriminalitätsphänomene werden mit ViCLAS untersucht?

    d) Hat ViCLAS Zusammenhänge zwischen einzelnen Verbrechen erkannt, und wenn ja, zwischen wie vielen in den letzten fünf Jahren?

    e) Wurde auch die Mordserie, die vom „Nationalsozialistischen Untergrund“ verantwortet wird, mit ViCLAS analysiert?

    f) Sofern ViCLAS Zusammenhänge findet, wie wird dann innerhalb des BKA weiter verfahren?

23. In welcher Form soll die Zusammenarbeit zwischen Landes- und Bundesbehörden sowie weiteren Akteuren innerhalb des „Kompetenzzentrums Informationstechnische Überwachung“ (ITÜ) erfolgen?

    a) In welcher Höhe soll das ITÜ im Jahr 2012 mit Finanzmitteln ausgestattet werden?

    b) In welcher Höhe sind finanzielle Mittel für die Programmierung von Computerspionageprogrammen (staatliche Trojaner) vorgesehen?

    c) Welche Akteure (Ämter, Behörden, Institute, Firmen, Stiftungen etc.) werden in deren Entwicklung eingebunden?

    d) Wie ist eine Kontrolle des Kompetenzzentrums bislang vorgesehen?

    e) Auf welche Art und Weise sollen von Bundesbehörden Programme zur Quellen-TKÜ zukünftig auf dem Zielsystem installiert werden, und auf welche Art und Weise geschah dies bislang?

24. Über welche technischen Funktionalitäten, insbesondere zur Erkennung von Gesichtern, verfügt die von Bundesbehörden laut der Antwort auf die Schriftliche Frage 15 auf Bundestagsdrucksache 17/8102 genutzte Software?

    a) In wie vielen Fällen wurde bereits Software der Firma Cognitech oder anderer Hersteller genutzt, um Lichtbilder mit der Inpol-Datenbank abzugleichen bzw. sofern hierfür keine Statistik existiert, in welcher Größenordnung bewegt sich die Praxis?

    b) Wie hoch ist die Trefferquote derart abgefragter Identifizierung?

    c) Mit welchen forensischen Anwendungen welcher Hersteller arbeiten Bundesbehörden bezüglich der Rekonstruktion unkenntlich gemachter Gesichter?

25. Mit welcher Technologie sind die 52 Beweissicherungs- und Dokumentationskraftwagen (BeDoKw) ausgestattet, die von den Firmen Gero, Elettronica und Vidit Systems gefertigt wurden und deutschen Bereitschaftspolizeien der Länder in Anwesenheit der Bundespolizei und des Beschaffungsamtes des Bundesministeriums des Innern überreicht wurden?

    a) Wie ist die Bundesregierung in die Organisation und Durchführung der Beschaffung eingebunden?

    b) Welche Produkte der Firmen Vidit, Geroh und Elettronica wurden verbaut?

c) Welche „Elektro- und IuK-Ausstattung“ (ausschreibungen.dgmarket.com/tenders/np-notice.do~5840668) anderer Hersteller wurden ausgeliefert, um Lageinformationen „visuell und akustisch aufzuzeichnen, zu selektieren, zu analysieren und bei Bedarf an übergeordnete Stellen zu übermitteln“ (tinyurl.com/c6uthg2)?

d) Mittels welcher Verfahren werden „alle gesammelten Daten“ im Fahrzeug verarbeitet und übermittelt?

e) Welche weiteren „Fähigkeiten“ können angesichts des “modularen Aufbaus“ integriert werden, und welche Überlegungen wurden hierfür angestellt?

f) Welche andere Firma hatte sich außer Elettronica um die Fertigung der Fahrzeuge beworben, und wieso wurde Elettronica bevorzugt?

Berlin, den 19. Dezember 2011

Dr. Gregor Gysi und Fraktion



Gesamtherstellung: H. Heenemann GmbH & Co., Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333